Ex: ① Compute $\gcd(222, 30)$ via Euclid's Algorithm.

② Express $\gcd(222, 30) = 222s + 30t$ for some $s, t \in \mathbb{Z}$.

Sol:

$222 = 30 \cdot 7 + 12 \quad \rightsquigarrow \quad 12 = 222(1) + 30(-7)$

$30 = 12 \cdot 2 + 6 \quad \rightsquigarrow \quad 6 = 30(1) + 12(-2) \quad *$

$12 = 6 \cdot 2 + 0 \quad \times$

$\therefore \gcd(222, 30) = 6$

$6 = 30(1) + 12(-2)$

$= 30(1) + (222(1) + 30(-7))(-2)$

$= 30(1) + 222(-2) + 30(14)$

$= 222(-2) + 30(15)$ ∎

$F_{a+b+1} = F_{a+1} F_{b+1} + F_a F_b$ w/ $F_n = n^{th}$ fib. num.

---

② $A_n = A_{n-1} + A_{n-2} \qquad n \geq 0$

$\Rightarrow A_n = F_n A_1 + F_{n-1} A_0 \qquad \forall\, n \geq 1$

$\forall$ $A_n = F_{a+n+1}$

Solve: $30x \equiv 12 \mod 5$ ← no solutions.

$\gcd(30, 5) \neq 1 \ldots$

Point: 30 is NOT invertible mod 5

Solve: $5x \equiv 12 \mod 33$ for $0 \le x < 33$.

Sol: Apply Euclid's Ext. Alg to $5, 33$

$33 = 5 \cdot 6 + 3 \rightsquigarrow 3 = 33(1) + 5(-6)$

$5 = 3 \cdot 1 + 2 \rightsquigarrow 2 = 5(1) + 3(-1)$ ←

$3 = 2 \cdot 1 + 1 \rightsquigarrow 1 = 3(1) + 2(-1)$

$2 = \boxed{1} \cdot 2 + 0$

$\therefore \quad 1 = 3(1) + 2(-1)$

$= 3(1) + (5(1) + 3(-1))(-1)$

$= 3(2) + 5(-1)$

$= (33(1) + 5(-6))(2) + 5(-1)$

$= 5(-13) + 33(2)$

$\therefore \quad 1 = 5(-13) + 33(2) \equiv 5(-13) + 0 \cdot 2 = 5(-13) \mod 33$

$-13 \equiv 20 \mod 33$

$\therefore \quad \boxed{1}x \equiv \boxed{(-13)5}x \equiv (-13)12 = -156 \mod 33$

Moreover $-156 = 33(-5) + 9$

(sanity check: $-150 - 15 + 9 = -150 - 6 = -156$ ✓)

Hence $\boxed{x \equiv 9 \mod 33}$, so $x = 9$ is the desired solution ☺

$\square$

$5x = 12$ over $\mathbb{Q}$

$x = 5^{-1} \cdot \boxed{5x} = 5^{-1} \boxed{12}$

Ex: Prove $5 \mid F_{5k}$ for all $k \in \mathbb{N}$. ($F_0 = 0$)

pf: We proceed by strong induction on k.

Base Case: If $k=0$, Then $F_{5\cdot 0} = F_0 = 0 = 5 \cdot 0$,

So $5 \mid F_{5k}$ in this case

Induction Step: Assume the result holds for all $0 \leq m < k$.

Now we compute as follows:

$$\begin{aligned} F_{5k} &= F_{5k-1} + F_{5k-2} \\ &= \left(F_{5k-2} + F_{5k-3}\right) + F_{5k-2} \\ &= 2F_{5k-2} + F_{5k-3} \\ &= 2\left(F_{5k-3} + F_{5k-4}\right) + F_{5k-3} \\ &= 3F_{5k-3} + 2F_{5k-4} \\ &= 3\left(F_{5k-4} + F_{5k-5}\right) + 2F_{5k-4} \\ &= 5F_{5k-4} + 3F_{5k-5} \\ &= 5F_{5k-4} + 3F_{5(k-1)} \end{aligned}$$

By the inductive hypothesis, $F_{5(k-1)} = 5n$ for some $n \in \mathbb{Z}$. Hence we have

$$\begin{aligned} F_{5k} &= 5F_{5k-4} + 3F_{5(k-1)} \\ &= 5F_{5k-4} + 3 \cdot 5n \\ &= 5\left(F_{5k-4} + 3n\right) \end{aligned}$$

and $F_{5k-4} + n \in \mathbb{Z}$ by cbs.

Hence $5 \mid F_{5k}$ as desired. ☒

Correspondence Principle:

If A and B are sets s.t. every element of A corresponds uniquely with an elt of B (and vice versa), then $\#A = \#B$.

---

* $\#\mathcal{P}[n] = 2^n$
* # ordered k-subsets of $[n]$ $= \frac{n!}{(n-k)!}$

$$\{\text{permutations of } [n]\} \longleftrightarrow \{(\sigma, \tau) : \sigma \text{ ordered } k\text{-subset of } [n],\ \tau \text{ permutation of } [n]\setminus\sigma\}$$